

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEBRASKA**

JOHN CHACON and LEONARD  
BRADLEY, individually and on behalf  
of all others similarly situated,

Plaintiffs,

v.

NEBRASKA MEDICINE,

Defendant.

Case No. \_\_\_\_\_

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

**CLASS ACTION COMPLAINT**

Plaintiffs JOHN CHACON and LEONARD BRADLEY (“Plaintiffs”), individually and on behalf of all others similarly situated, bring this action against Defendant NEBRASKA MEDICINE (“NM” or “Defendant”), a Nebraska corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record:

**NATURE OF THE ACTION**

1. This class action arises out of the recent targeted cyber-attack at Defendant’s medical facilities that disrupted operations and among other things, allowed a third party to access Defendant’s computer systems and data, resulting in the removal of highly sensitive personal information and medical records of approximately 219,000 patients from Defendant’s computer network (the “Cyber-Attack”).

2. As a result of the Cyber-Attack, Plaintiffs and Class Members suffered ascertainable losses in the form of loss of the value of their private and confidential information,

loss of the benefit of their contractual bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

3. Plaintiffs' and Class Members' sensitive personal information—which was entrusted to Defendant, its officials, and agents—was compromised, unlawfully accessed, and stolen due to the Cyber-Attack. Information compromised in the Cyber-Attack includes names, date of birth, Social Security numbers, Medicaid ID numbers, date of last visit, admission date, discharge date, diagnosis code, other protected health information as defined by the HIPAA, and additional personally identifiable information (“PII”) and protected health information (“PHI”) that Defendant collected and maintained (collectively the “Private Information”).

4. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

5. Defendant maintained the Private Information in a reckless manner.

6. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks of the type that cause actual disruption to Plaintiffs' and Class Members' medical care and treatment.

7. Upon information and belief, the mechanism of the cyber-attack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known and foreseeable risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. In addition, Defendant and its employees failed to properly monitor the computer

network and systems that housed the Private Information.

9. Had Defendant properly monitored its property, it would have discovered the intrusion sooner.

10. Because of the Cyber-Attack, Plaintiffs and Class Members suffered injury and damages in the form of theft and misuse of their Private Information.

11. What's more, Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

12. Armed with the Private Information accessed in the Cyber-Attack, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

13. As a further result of the Cyber-Attack, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

14. Plaintiffs and Class Members have and may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

15. As a direct and proximate result of the Cyber-Attack and subsequent data breach, Plaintiffs and Class Members have suffered and will continue to suffer damages and economic losses in the form of: 1) the loss of time needed to: take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits, charges, and fees charged against their accounts; and deal with spam messages and e-mails received as a result of the Data Breach. Plaintiffs and Class Members have likewise suffered and will continue to suffer an invasion of their property interest in their own PII and PHI such that they are entitled to damages for unauthorized access to and misuse of their PII and PHI from Defendant. And, Plaintiffs and Class Members will suffer from future damages associated with the unauthorized use and misuse of their PII and PHI as thieves will continue to use the stolen information to obtain money and credit in their name for several years.

16. Per the Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or removed from the network during the Cyber-Attack.

17. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

18. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct asserting claims for negligence, an intrusion upon seclusion, breach of implied contract, breach of fiduciary duty, breach of the Nebraska Consumer Protection Act ("CPA"), Nebraska Revised Statutes § 59-1601, *et seq.*, and violation of the Nebraska Uniform Deceptive

Trade Practices Act (“UDTPA”), Nebraska Revised Statutes § 87-302(a)(5),(8) and (15).

### **PARTIES**

19. Plaintiff John Chacon is, and at all times mentioned herein was, an individual citizen of the State of Iowa residing in Carter Lake, Iowa. Plaintiff Chacon was and is a patient of Defendant. Plaintiff Chacon received notice from NM that the Data Breach had occurred following an attack on NM’s computer systems, and that his personal data was involved. A copy of the notice is attached hereto as **Exhibit A**.

20. Plaintiff Leonard Bradley is, and at all times mentioned herein was, an individual citizen of the State of Nebraska residing in Omaha, Nebraska. Plaintiff Bradley was a patient of Defendant. Plaintiff Bradley received notice from NM that the Data Breach had occurred following an attack on NM’s computer systems, and that his personal data was involved. A copy of the notice is attached hereto as **Exhibit B**.

21. Defendant Nebraska Medicine is a Nebraska non-profit corporation with its principal place of business at 987400 Nebraska Medical Center, Omaha, Nebraska 68198-7400.

### **JURISDICTION AND VENUE**

22. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members, the aggregated claims of the individual Class Members exceed the sum or value of \$5,000,000 exclusive of interest and costs, and Plaintiff Chacon and Members of the proposed Class are citizens of states different from Defendant.

23. This Court has jurisdiction over Defendant, which operates and is headquartered in this District. The computer systems implicated in this Cyber-Attack are also likely based in this District. Through its business operations in this District, NM intentionally avails itself of the

markets within this District to render the exercise of jurisdiction by this Court just and proper.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District. Defendant is a Nebraska corporation headquartered in this District, where it maintains personally PII and PHI of its current and former patients, and has caused harm to Plaintiffs and Class Members, some of whom reside in this District.

### **FACTUAL ALLEGATIONS**

#### ***Defendant's Business***

25. Nebraska Medicine bills itself as the most comprehensive health network in the Omaha, Nebraska region, with two major hospitals, more than 1000 doctors and 40 clinics in the Omaha area. Patients are seen by Nebraska Medicine specialists from all 50 states and from 47 countries.

26. Nebraska Medicine further advertises that it is the region's only 24/7 trauma center providing comprehensive care for adults and children, a regional leader in cardiovascular and neurosciences, and that it has an international reputation in oncology, transplant, and biocontainment.

27. Nebraska Medicine is a "\$1.8 billion academic health system" with 8,000-9,000 employees, and more than 1,000 affiliated physicians. It is the primary clinical partner of the University of Nebraska Medical Center.

28. Nebraska Medicine operates out of multiple facilities, including: two hospitals, anchored by tertiary/quaternary academic medical center, Nebraska Medical Center; 39 specialty and primary care clinics, offering 50 specialties and subspecialties; partial ownership of two rural hospitals and one specialty hospital.

29. The two hospitals have 809 licensed beds in Omaha and Bellevue—718 beds at Nebraska Medical Center and another 91 beds at Bellevue Medical Center. There are 36 operating rooms at the various facilities operated by Nebraska Medicine.

30. Nebraska Medicine sees a staggering number of patients, with 33,606 discharges, 1.06 million outpatient visits (primary and specialty), and 95,040 ER visits.

31. In the ordinary course of receiving medical care and treatment from Defendant, patients are required to provide (and Plaintiffs did in fact provide) Defendant with sensitive, personal, and private information such as:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Information relating to individual medical history;
- Insurance information and coverage;
- Information concerning an individual's doctor, nurse or other medical providers;
- Photo identification;
- Employer information; and
- Other information that may be deemed necessary to provide care.

32. Plaintiffs and Class Members were required to give Defendant this information as a condition of receiving medical treatment from NM.

33. Defendant also gathers certain medical information about patients and creates records of the care it provides to them.

34. Additionally, Defendant may receive private and personal information from other individuals and/or organizations that are part of a patient's "circle of care", such as referring physicians, patients' other doctors, patient's health plan(s), close friends, and/or family members.

35. Nebraska Medicine publicly recognizes and affirms its duties and responsibilities to keep its patients' personal information private and confidential. In its "Patients Rights and Responsibilities," posted on its website, NM states:

### **3. Privacy and Confidentiality**

All information about you will be kept confidential, including the privacy of your health information. The Notice of Privacy Practices explains how your health information may be used.<sup>1</sup>

36. Nebraska Medicine also publishes a Notice of Privacy Practices ("Privacy Notice") that applies to the following organizations and clinics:

- The Nebraska Medical Center and its medical staff, including academic and private practice physicians, and allied health professionals while providing services at these locations, as an organized health care arrangement;
- The Bellevue Medical Center and its medical staff and allied health professionals as an organized healthcare arrangement;
- University of Nebraska Medical Center ("UNMC");
- UNMC Physicians;
- Nebraska Pediatric Practice, Inc.; and
- University Dental Associates ("UDA").

All of these organizations use and distribute the Privacy Notice as their Joint Notice of Privacy Practices and follow the information practices described in the Privacy Notice when using or disclosing records or information.

---

<sup>1</sup> <https://www.nebraskamed.com/patients/rights-responsibilities> (last accessed Feb. 22, 2021).

37. Upon information and belief, a copy of the Privacy Notice is provided to each patient upon registration at one of NM's facilities, and copies of the Privacy Notice were provided to the Plaintiffs.

38. The Privacy Notice recognizes NM's legal duties to protect the privacy and confidentiality of patient data, including that of Plaintiffs and Class Members.

39. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its patients, the Privacy Notice further promises that NM: 1) will "[m]aintain the privacy of your health information during your lifetime and for 50 years following your death;" 2) will "[p]rovide you with an additional current copy of our Notice upon request;" 3) will "[a]bide by the terms of our current Notice;" 4) will "[n]otify you following a breach of unsecured protected health information in the event you are affected," and; 5) "will not use or disclose your health information without your written authorization, except as described in this Notice."<sup>2</sup>

### ***The Data Breach***

40. Between August 27, 2020 and September 20, 2020, Defendant NM experienced a targeted cybersecurity incident where cyberthieves had unauthorized access to NM's network for approximately 24 days.<sup>3</sup>

41. Upon information and belief, the cyber-attack was targeted at Defendant, due to Defendant's status as a healthcare entity that collects, creates, and maintains both PII and PHI. The targeted cyber-attack was expressly designed to gain access to private and confidential data,

---

<sup>2</sup> <https://www.nebraskamed.com/patients/rights-responsibilities/notice-privacy-practices> (last accessed Feb. 22, 2021).

<sup>3</sup> <https://www.healthcareinfosecurity.com/notification-breach-affecting-219000-delayed-a-15986> (last accessed Feb. 22, 2021)

including (among other things) the PII and PHI of patients like Plaintiffs and Class Members.

42. NM did not discover that unauthorized persons had gained access to its computer systems for over three weeks, and only became aware of the unauthorized access when it identified “unusual network activity” affecting some of its IT systems on September 20, 2020.

43. The cyberthieves infected Defendant’s IT systems with malicious software (aka malware), and acquired copies of patient and employee information held on Defendant’s systems.

44. The patient data that was exposed included patients who were treated at Nebraska Medicine/University of Nebraska Medical Center (“UNMC”), and three other healthcare organizations—Faith Regional Health Services, Great Plains Health, and Mary Lanning Healthcare—whose information was in the NM network that was compromised.

45. After exfiltrating (aka stealing) patient data, upon information and belief, the cyberthieves launched a ransomware attack using the malware with which the thieves had infected NM’s systems. This ransomware attack caused disruption to NM’s operations, requiring Defendant to initiate its “incident response protocols to minimize any disruption to patients,” to isolate potentially impacted devices, and to shut off select systems as a precaution.

46. Defendant hired forensic experts to perform an investigation into the full nature and scope of the cyber-attack. The investigation found that cyber-criminals had been able to access patient data that included names, addresses, dates of birth, health insurance information, medical record number, and/or clinical information (including physician notes, laboratory results, imaging, diagnosis information, treatment information, and/or prescription information) and Social Security numbers.<sup>4</sup>

47. Despite learning of the Cyber-Attack on or about September 20, 2020, Defendant

---

<sup>4</sup> <https://www.unmc.edu/privacy-incident/> (last accessed Feb. 22, 2021).

only provided notice of the data breach to its patients beginning on February 5, 2021, in derogation of Nebraska's Data Breach Notification law (the Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006), Nebraska Revised Statutes § 87-801, *et seq.*, which requires notice as soon as possible and without unreasonable delay.

48. Notably, the Notice Letters sent out to Plaintiffs and Class Members contained far less information than the "Privacy Incident" notification that Defendant posted on its website. The notice on the website stated this:

On September 20, 2020, we identified unusual network activity that affected some of our IT systems. Immediately upon learning of this incident, we initiated our incident response protocols to minimize any disruption to patients, isolated potentially impacted devices, and shut off select systems as a precaution. We also initiated an investigation, computer forensic experts were engaged to assist our ongoing investigation, and we notified law enforcement.

After a comprehensive evaluation, we confirmed that an unauthorized person gained access to select systems on our network between August 27, 2020 and September 20, 2020. During that time, the unauthorized person deployed malware and acquired copies of some patient and employee information held on those systems. This incident also impacted a limited number of patients seen at Faith Regional Health Services, Great Plains Health, and Mary Lanning Healthcare whose information was in the Nebraska Medicine/UNMC network. For a limited number of Nebraska Medicine/UNMC patients, this information included one or more of their name, address, date of birth, health insurance information, medical record number, and/or clinical information, which may have included physician notes, laboratory results, imaging, diagnosis information, treatment information, and/or prescription information. For a limited number of patients, Social Security numbers were also impacted. Importantly, this incident did not result in unauthorized access to Nebraska Medicine and UNMC's electronic medical record application.

We began mailing notification letters to impacted patients for whom we have an address on February 5, 2021, which provided guidance on how they can help protect their information.<sup>5</sup>

49. By contrast the Notice Letter sent out to affected patients like Plaintiff Chacon

---

<sup>5</sup> <https://www.unmc.edu/privacy-incident/> (last accessed Feb. 22, 2021).

stated:

On September 20, 2020, we identified unusual network activity. We immediately took steps to secure the network and began an investigation with the assistance of a computer forensic firm. The investigation determined that an unauthorized person gained access to our network between August 27, 2020 and September 20, 2020. During that time, the unauthorized person deployed malware and acquired copies of some of the information on our systems. On September 24, 2020, we determined that the unauthorized person acquired copies of documents that contained patient information. We conducted a review of all documents involved and determined that one or more files contained your information. This may have included your name, address, date of birth, health insurance information, medical record number, and/or clinical information, which may have included physician notes, laboratory results, imaging, diagnosis information, treatment information, and/or prescription information.

*See Exhibit A.*

50. Outside experts have criticized Defendant for its delay in notifying patients, and for downplaying the risk. Kate Borten, president of the privacy and security consulting firm The Marblehead Group, stated:

“Notification was long past the HIPAA-required 60 days, and the organization does not provide an explanation . . . Notification delay raises the risk of harm to patients . . . If patients are unaware that their information has been compromised, they cannot take protective steps.”

Borten went on to note that the data compromised in this breach appears to be highly sensitive, and that NM downplayed the risks:

“The organization attempts to reassure patients by stating that the electronic medical record system was not breached. This is disingenuous since the crucial point is what data was affected, not which system . . . [the notification] downplays the risk and could mislead patients so they do not take the breach seriously.”<sup>6</sup>

51. The Notice Letters sent to Plaintiffs downplayed the risks associated with this large and serious data breach even more, as they provided substantially less information to Plaintiffs.

52. Upon information and belief, Notice Letters were sent to approximately 219,000

---

<sup>6</sup> <https://www.healthcareinfosecurity.com/notification-breach-affecting-219000-delayed-a-15986> (last accessed Feb. 22, 2021).

persons, and was reported to the U.S. Department of Health and Human Services (“HHS”) on November 23, 2020.

53. Based on the Notice of Data Breach letters they received (Exhibits A and B to this Complaint), which inform Plaintiffs that their Private Information was removed from Defendant’s network and computer systems, Plaintiffs believe their Private Information was stolen from Defendant’s network (and subsequently sold) in the Cyber-Attack.

54. Further, the removal of the Private Information from Defendant’s system—information that included full names, dates of birth, and Social Security numbers (which are the keys to identity theft and fraud)—demonstrates that this Cyber-Attack was targeted.

55. Cyber-attacks against healthcare organizations such as Defendant are targeted. According to the 2019 Health Information Management Systems Society, Inc. (“HIMMS”) Cybersecurity Survey, “[a] pattern of cybersecurity threats and experiences is discernable across US healthcare organizations. Significant security incidents are a near-universal experience in US healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets.”<sup>7</sup> “Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From Social Security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.”<sup>8</sup>

56. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiffs and Class Members, to keep their Private

---

<sup>7</sup> <https://www.himss.org/himss-cybersecurity-survey> (last accessed Dec. 10, 2020).

<sup>8</sup> <https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last accessed June 20, 2020).

Information confidential and to protect it from unauthorized access and disclosure.

57. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

58. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the healthcare industry preceding the date of the breach.

59. Data breaches, including those perpetrated against the healthcare sector of the economy, have become widespread.

60. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.<sup>9</sup>

61. Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.<sup>10</sup>

62. The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.<sup>11</sup>

63. Indeed, cyber- attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware

---

<sup>9</sup> [https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020\\_ITRC\\_2019-End-of-Year-Data-Breach-Report\\_FINAL\\_Highres-Appendix.pdf](https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf) (last accessed Dec. 10, 2020).

<sup>10</sup> *Id.*

<sup>11</sup> *Id.* at 15.

criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”<sup>12</sup>

64. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including Defendant.

***Defendant Fails to Comply with FTC Guidelines***

65. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

66. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

67. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords

---

<sup>12</sup> [https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl\\_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm\\_source=newsletter&utm\\_medium=email&utm\\_campaign=consumerprotection](https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection) (last accessed Dec. 10, 2020).

to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

68. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

69. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In re Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at \*32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”).

70. Defendant failed to properly implement basic data security practices. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

71. Defendant was at all times fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

### ***Defendant Fails to Comply with Industry Standards***

72. As shown above, experts studying cyber security routinely identify healthcare

providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

73. Experts in the healthcare industry assert that “data breaches cost the healthcare industry approximately \$5.6 billion every year[.]”

74. According to the University of Illinois Chicago (“UIC”), “To improve cybersecurity in health care, organizations need to hire informatics professionals who can not only collect, manage and leverage data, but protect it as well.”<sup>13</sup>

75. UIC has identified several strategies and best practices that, at a minimum, should be implemented by healthcare providers like Defendant, including but not limited to: establishing a security culture; protecting mobile devices; thoroughly educating all employees; strong passwords that need to be changed regularly; multi-layer security, including firewalls, anti-virus, and anti-malware software; limit network access; control physical access to devices; encryption, making data unreadable without a password or key; multi-factor authentication; backup data, and; limiting employees access to sensitive and protected data.<sup>14</sup>

76. A number of industry and national best practices have been published and should be used as a go-to resource when developing an institution’s cybersecurity standards. The Center for Internet Security (“CIS”) released its Critical Security Controls, and all healthcare institutions are strongly advised to follow these actions.<sup>15</sup>

77. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network

---

<sup>13</sup> See *Cybersecurity: How Can It Be Improved in Health Care?*, Health Informatics-University of Illinois Chicago (last viewed Dec. 9, 2020), <https://healthinformatics.uic.edu/blog/cybersecurity-how-can-it-be-improved-in-health-care/>.

<sup>14</sup> *Id.*

<sup>15</sup> <https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/> (last accessed Dec. 10, 2020)

ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

78. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

79. These foregoing frameworks are existing and applicable industry standards in Defendant's industry.

***Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security***

80. Defendant Nebraska Medicine is a "covered entity" under HIPAA.

81. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

82. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

83. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules

include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

84. Defendant's Cyber-Attack resulted from a combination of insufficiencies that demonstrate it failed to comply with safeguards mandated by HIPAA regulations.

***Defendant's Breach***

85. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard the NM computer systems, network, and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Failing to adequately protect patients' Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;
- d. Failing to apply all available security updates;
- e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;
- f. Failing to practice the principle of least-privilege and maintain credential hygiene;
- g. Failing to avoid the use of domain-wide, admin-level service accounts;
- h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords;

- i. Failing to properly train and supervise employees in the proper handling of inbound emails;
- j. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- k. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- l. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- m. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- n. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- o. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- p. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

- q. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or
- r. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR 164.304 definition of encryption).

86. As the result of computer systems in dire need of security upgrading and inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiffs’ and Class Members’ Private Information.

***Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft***

87. Cyber-attacks at medical facilities such as Defendant’s are especially problematic because of the disruption they cause to the medical care and treatment and overall daily lives of patients affected by the attack.

88. For instance, loss of access to patient histories, charts, images and other information forces providers to limit or cancel patient treatment because of the disruption of service.

89. This leads to a deterioration in the quality of overall care patients receive at facilities affected by cyber-attacks and related data breaches.

90. Researchers have found that at medical facilities that experienced a data security

incident, the death rate among patients increased in the months and years after the attack.<sup>16</sup>

91. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in patient outcomes, generally.<sup>17</sup>

92. Similarly, cyber-attacks and related data security incidents inconvenience patients. Inconveniences patients encounter as a result of such incidents include, but are not limited, to the following:

- a. rescheduling medical treatment;
- b. finding alternative medical care and treatment;
- c. delaying or foregoing medical care and treatment;
- d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and
- e. losing patient medical history.<sup>18</sup>

93. Cyber-attacks that result in the removal of protected data are also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

A breach under the HIPAA Rules is defined as, “. . . the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.” *See* 45 C.F.R. 164.40

94. Data breaches represent a significant problem for patients who have already

---

<sup>16</sup> *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019) <https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks> (last accessed Dec. 10, 2020).

<sup>17</sup> *See Data Breach Remediation Efforts and Their Implications for Hospital Quality*, Health Services Research <https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203> (last accessed Dec. 10, 2020).

<sup>18</sup> *See, e.g.,* <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/> (last accessed Dec. 10, 2020); <https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech> (last accessed on Dec. 10, 2020).

experienced inconvenience and disruption associated with a cyber-attack.

95. The United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”<sup>19</sup>

96. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.<sup>20</sup>

97. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

98. Identity thieves can also use Social Security numbers to obtain a driver’s license or official identification card in the victim’s name but with the thief’s picture; use the victim’s name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim’s information.

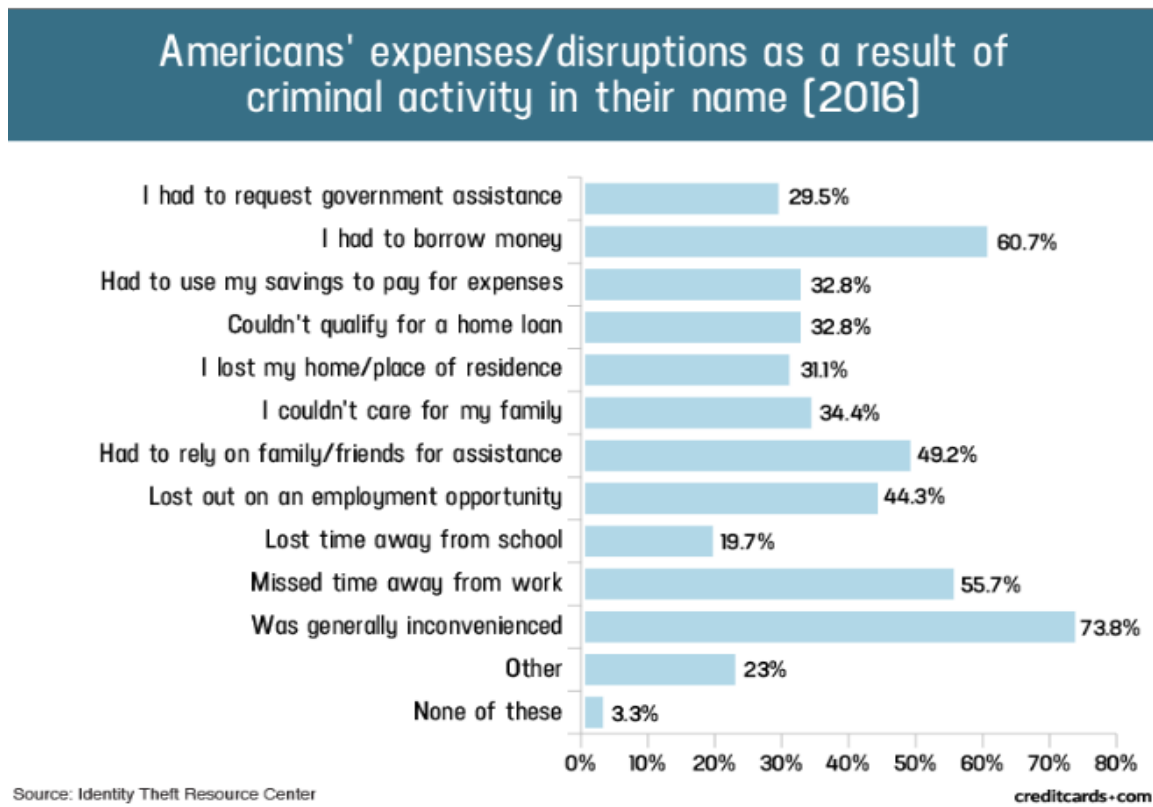
99. In addition, identity thieves may obtain a job using the victim’s Social Security number, rent a house or receive medical services in the victim’s name, and may even give the victim’s personal information to police during an arrest resulting in an arrest warrant being issued in the victim’s name.

---

<sup>19</sup> See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Gov’t Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited Apr. 12, 2019) (“GAO Report”).

<sup>20</sup> See <https://www.identitytheft.gov/Steps> (last visited Dec. 8, 2020).

100. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:<sup>21</sup>



101. What's more, theft of Private Information is also gravely serious. PII/PHI is a valuable property right.<sup>22</sup>

102. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

<sup>21</sup> See Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> (last accessed Dec. 10, 2020).

<sup>22</sup> See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at \*3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

103. Theft of PHI, in particular, is gravely serious: “A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”<sup>23</sup>

104. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds’ medical insurance premiums.

105. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

*See* GAO Report, at p. 29.

106. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years.

107. Where the most private information belonging to Plaintiffs and Class Members was

---

<sup>23</sup> *See* Medical Identity Theft, Federal Trade Commission Consumer Information (last visited Dec. 9, 2020), <http://www.consumer.ftc.gov/articles/0171-medical-identity-theft>.

accessed and removed from Defendant's network, there is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

108. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

109. While credit card information can sell for as little as \$1-\$2 on the black market, other more sensitive information can sell for as much as \$363 according to the Infosec Institute. PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

110. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200.

111. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

112. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities

is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

113. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."<sup>24</sup>

114. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."<sup>25</sup>

115. Medical information is especially valuable to identity thieves. The asking price on the Dark Web for medical data is \$50 and up.<sup>26</sup>

116. Because of its value, the medical industry has experienced disproportionately higher numbers of data theft events than other industries.

---

<sup>24</sup> *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited October 28, 2020).

<sup>25</sup> *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited October 28, 2020).

<sup>26</sup> See Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), <https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/> (last accessed Dec. 10, 2020).

117. Defendant therefore knew or should have known this risk and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

***Plaintiffs' and Class Members' Damages***

118. To date, Defendant has done absolutely nothing to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Cyber-Attack and data breach, including, but not limited to, the costs and loss of time they incurred because of the disruption of service at Defendant's medical facilities. Nebraska Medicine has only offered inadequate identity monitoring services to certain affected individuals (based upon the type of data stolen), and has not offered any credit monitoring or identity theft protection to a vast number of persons whose data was compromised in the Cyber-Attack.

119. Moreover, the 12 months of credit monitoring offered to certain persons whose private information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

120. Defendant entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII and PHI.

121. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Cyber-Attack.

122. As a direct and proximate result of Defendant's conduct, Plaintiff Chacon receives multiple scam phone calls per week—calls that he was not receiving prior to the Cyber-Attack. The scam calls appear to be placed with the intent of reverse engineering his identity.

123. As a direct and proximate result of Defendant's conduct, all Plaintiffs and Class

Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

124. Plaintiff Bradley has been placed at the imminent, immediate, and continuing risk of harm through the theft of his name, date of birth, and Social Security number, which are the keys to financial fraud, and also through the theft of his PHI (including his clinical information).

125. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

126. Plaintiffs and Class Members have been, and face substantial risk of being targeted in the future, subjected to phishing, data intrusion, and other illegal schemes (like the scam phone calls received by Plaintiff Chacon) based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

127. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Cyber-Attack.

128. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Cyber-Attack. Numerous courts have recognized the propriety of loss of value damages in related cases.

129. Class Members were also damaged via benefit-of-the-bargain damages, in that they overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and Plaintiffs' and Class Members' Private Information. Thus, Plaintiffs and the Class Members did not get what they paid for.

130. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial and medical accounts and records for misuse.

131. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Cyber-Attack.

132. In addition to the loss of use of and access to their medical records and costs associated with the inability to access their medical records (including actual disruption of medical care and treatment), many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Cyber-Attack relating to:

- a. Finding alternative medical care and treatment;
- b. Delaying or foregoing medical care and treatment;
- c. Undergoing medical care and treatment without medical providers having access to a complete medical history and records;
- d. Having to retrace or recreate their medical history;
- e. Finding fraudulent charges;
- f. Canceling and reissuing credit and debit cards;
- g. Purchasing credit monitoring and identity theft prevention;
- h. Addressing their inability to withdraw funds linked to compromised accounts;
- i. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
- j. Placing “freezes” and “alerts” with credit reporting agencies;
- k. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

- l. Contacting financial institutions and closing or modifying financial accounts;
- m. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;
- n. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and
- o. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

133. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

134. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

135. Plaintiffs and Class members were also injured and damaged by the delayed notice of this data breach, as it exacerbated the imminent risk of harm by leaving Plaintiffs and Class Members without the knowledge that would have enabled them to take proactive steps to protect themselves.

136. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an

increased risk of future harm.

### **CLASS ACTION ALLEGATIONS**

137. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

138. Plaintiffs bring this action individually and on behalf of all other persons similarly situated (“the Class”) pursuant to Federal Rule of Civil Procedure 23.

139. Plaintiffs propose the following Class definition(s), subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiffs bring this action and seeks certification of the following Class:

All persons whose PII and/or PHI was compromised as a result of the Cyber-Attack that Nebraska Medicine discovered on or about September 20, 2020, and who were sent notice of the Data Breach.

140. Excluded from the Class are Defendant’s officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

141. Plaintiffs reserve the right to amend the definitions of the Class or add a Class if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

142. Certification of Plaintiffs’ claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

143. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time,

based on information and belief, the Class consists of over 219,000 patients of Defendant NM whose data was compromised in the Cyber-Attack and data breach.

144. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a) Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;
- b) Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Cyber-Attack;
- c) Whether Defendant's data security systems prior to and during the Cyber-Attack complied with applicable data security laws and regulations including, *e.g.*, HIPAA;
- d) Whether Defendant's data security systems prior to and during the Cyber-Attack were consistent with industry standards;
- e) Whether Defendant owed a duty to Class Members to safeguard their Private Information;
- f) Whether Defendant breached their duty to Class Members to safeguard their Private Information;
- g) Whether computer hackers obtained Class Members' Private Information in the Cyber-Attack;
- h) Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

- i) Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j) Whether Defendant owed a duty to provide Plaintiffs and Class Members notice of this data breach, and whether Defendant breached that duty;
- k) Whether Defendant's conduct was negligent;
- l) Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;
- m) Whether Defendant's actions violated federal law;
- n) Whether Defendant's acts violated Nebraska law; and
- o) Whether Plaintiffs and Class Members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

145. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Cyber-Attack.

146. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Classes. Plaintiffs' Counsel are competent and experienced in litigating class actions.

147. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and

desirable advantages of judicial economy.

148. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

149. Defendant has acted on grounds that apply generally to the Classes as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

## **CAUSES OF ACTION**

### **COUNT I**

#### **NEGLIGENCE**

#### **(On Behalf of Plaintiffs and All Class Members)**

150. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 149 above as if fully set forth herein.

151. Defendant required Plaintiffs and Class Members to submit non-public personal information in order to obtain medical services.

152. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and

safeguard its computer property—and Class Members’ Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant’s duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

153. Under Nebraska Revised Statutes § 87-808, Defendant owed a duty to protect personal information from unauthorized access, acquisition, use, or disclosure, a duty to implement and maintain reasonable security procedures and practices that are appropriate to the nature and sensitivity of the personal information it maintains, and a duty to comply with HIPAA regulations governing data security and privacy.

154. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

155. Defendant’s duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its client patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

156. Defendant’s duty to use reasonable security measures under HIPAA required Defendant to “reasonably protect” confidential data from “any intentional or unintentional use or disclosure” and to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” 45 C.F.R. § 164.530(c)(1).

157. Some or all of the medical information at issue in this case constitutes “protected health information” within the meaning of HIPAA.

158. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

159. Defendant’s duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

160. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members’ Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members’ Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members’ Private Information;
- e. Failing to detect in a timely manner that Class Members’ Private Information had been compromised;
- f. Failing to timely notify Class Members about the Cyber-Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

- g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

161. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the medical industry.

162. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

163. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Cyber-Attack and data breach.

164. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

**COUNT II**  
**INVASION OF PRIVACY BY TRESPASS OR INTRUSION**  
**(On Behalf of Plaintiffs and All Class Members)**

165. Plaintiffs repeat and re-allege each and every allegation contained in Paragraphs 1 through 149 as if fully set forth herein.

166. The State of Nebraska enacted into law the tort of Invasion of Privacy; trespass or intrude upon a person's solitude. Nebraska Revised Statutes § 20-203.

167. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

168. By intentionally failing to keep Plaintiffs' and Class Members' Private Information

safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs' and Class Members' privacy by intrusion.

169. Defendant knew that an ordinary person in Plaintiffs' or a Class Member's position would consider this invasion of privacy and Defendant's intentional actions highly offensive and objectionable to reasonable persons.

170. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

171. Defendant intentionally concealed from Plaintiffs and Class Members an incident that misused and/or disclosed their Private information without their informed, voluntary, affirmative, and clear consent.

172. In failing to protect Plaintiffs' and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

173. Plaintiffs sustained damages (as outlined above) as a direct and proximate consequence of the invasion of their privacy by intrusion, and therefore seek an award of general damages for harm to Plaintiffs' and Class Members' interest on behalf of themselves and the Class, damages for mental suffering, special damages, and if none of these are proven, nominal damages.

**COUNT III**  
**BREACH OF IMPLIED CONTRACT**  
**(On Behalf of Plaintiffs and All Class Members)**

174. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 149 above

as if fully set forth herein.

175. Through their course of conduct, Defendant, Plaintiffs, and Class Members entered into implied contracts for the provision of medical care and treatment, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

176. Specifically, Plaintiffs entered into a valid and enforceable implied contract with Defendant when they first went for medical care and treatment at one of Defendant's facilities.

177. The valid and enforceable implied contracts to provide medical care and treatment services that Plaintiffs and Class Members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant creates on its own from disclosure.

178. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

179. Defendant solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

180. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

181. Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

182. Under the implied contracts, Defendant and/or its affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiffs and Class Members; and (b) protect Plaintiffs' and the Class Members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

183. Both the provision of medical services healthcare and the protection of Plaintiffs' and Class Members' Private Information were material aspects of these implied contracts.

184. The implied contracts for the provision of medical services—contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice.

185. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

186. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiffs and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, or entrusted their Private Information to Defendant in the absence

of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

187. A meeting of the minds occurred, as Plaintiffs and Members of the Class agreed to and did provide their Private Information to Defendant and/or its affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

188. Plaintiffs and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

189. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Cyber-Attack.

190. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by its notifications of the Cyber-Attack to Plaintiffs and approximately 219,000 Class Members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiffs' and the Class Members' Private Information, as set forth above.

191. The Cyber-Attack was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

192. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that

described in the contracts. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

193. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

194. As a direct and proximate result of the Cyber-Attack/data breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

195. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Cyber-Attack/data breach.

196. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**COUNT IV**  
**BREACH OF FIDUCIARY DUTY**  
**(On Behalf of Plaintiffs and All Class Members)**

197. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 149 above as if fully set forth herein.

198. In providing their Private Information to Defendant, Plaintiffs and Class Members justifiably placed special confidence in Defendant to act in good faith and with due regard to interests of Plaintiffs and Class Members to safeguard and keep confidential that Private Information.

199. Defendant NM accepted the special confidence placed in it by Plaintiffs and Class Members, as evidenced by its assertion that it is “respects the needs of clients for confidentiality, privacy, and security” and by the promulgation of its Privacy Notice. There was an understanding between the parties that Defendant would act for the benefit of Plaintiffs and Class Members in preserving the confidentiality of the Private Information.

200. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardians of Plaintiffs’ and Class Members’ Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members, for the safeguarding of Plaintiffs’ and Class Members’ Private Information.

201. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its patients’ relationship, in particular, to keep secure the Private Information of its patients.

202. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Cyber-Attack and data breach in a reasonable and practicable period of time.

203. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs’ and Class Members’ Private Information.

204. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Cyber-Attack and data breach.

205. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

206. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

207. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

208. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

209. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

210. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in

violation of 45 C.F.R. § 164.306(a)(3).

211. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

212. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

213. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to effectively train all Members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the Members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

214. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

215. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

216. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated

with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Cyber-Attack and data breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Cyber-Attack and data breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

217. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

**COUNT V**  
**VIOLATION OF NEBRASKA CONSUMER PROTECTION ACT**  
**Nebraska Revised Statutes § 59-1601, *et seq.***  
**(On Behalf of Plaintiffs and Class Members)**

218. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 149 above as if fully set forth herein.

219. Plaintiffs, Class Members, and Defendant each qualify as a person engaged in trade or commerce as contemplated by the Nebraska Consumer Protection Act ("CPA"), Neb. Rev. Stat. § 59-1601, *et seq.*

220. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of the CPA, including but not limited to:

- a. representing that its services were of a particular standard or quality that it knew or should have known were of another;
- b. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Class Members' Private Information, which was a direct and proximate cause of the Cyber-Attack and data breach;
- c. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Cyber-Attack and data breach;
- d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45 and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Cyber-Attack and data breach;
- e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Private Information, including by implementing and maintaining reasonable security measures;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Private Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Personal Information, including duties imposed

by the FTCA, 15 U.S.C. § 45 and HIPAA, 45 C.F.R. § 164, which was a direct and proximate cause of the Cyber-Attack and data breach.

221. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of NM's data security and ability to protect the confidentiality of consumers' Private Information.

222. In addition, Defendant's failure to secure consumers' PHI violated HIPAA and the FTCA and therefore violates the CPA.

223. Also, Defendant's failure to give timely notice of this Cyber-Attack in violation Nebraska's notification of security breach statute, Neb. Rev. Stat. § 87-801 *et seq* is an unfair or deceptive act pursuant to Neb. Rev. Stat. § 87-808, and therefore violates the Consumer Protection Act.

224. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PHI of Plaintiffs and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

225. The aforesaid conduct constitutes a violation of the CPA, Neb. Rev. Stat. § 59-1603, in that it is a restraint on trade or commerce.

226. These violations have caused financial injury to the Plaintiffs and the other Class Members.

227. The Defendant's violations of the CPA have an impact of great or general importance on the public.

228. As a direct and proximate result of Defendant's violation of the CPA, Plaintiffs and Class Members are entitled to a judgment under Neb. Rev. Stat. § 59-1609 to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable

attorney's fees), and such other further relief as the Court deems just and proper.

**COUNT VI**  
**VIOLATION OF NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT**  
**Nebraska Revised Statutes § 87-301, *et seq.***  
**(On Behalf of Plaintiffs and Class Members)**

229. Plaintiffs, all Class Members and Defendant each qualify as a person engaged in trade or commerce as contemplated by the Nebraska Uniform Deceptive Trade Practices Act (“UDTPA”), Neb. Rev. Stat. § 87-301, *et seq.*

230. Defendant's implied and express representations that it would adequately safeguard Plaintiffs' and Class Members' PII and PHI constitute representations as to characteristics, uses, or benefits of services that such services did not actually have, in violation of Neb. Rev. Stat. § 87-302(a)(5).

231. Defendant's implied and express representations that it would adequately safeguard Plaintiffs' and Class Members' PII and PHI constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Neb. Rev. Stat. § 87-302(a)(8).

232. Defendant knowingly made false or misleading statements in its privacy policy regarding the use of personal information submitted by members of the public (*i.e.*, the Privacy Notice referenced above, published on the Nebraska Medicine website and otherwise distributed or published), in that Defendant did not “[m]aintain the privacy of your health information,” in violation of Neb. Rev. Stat. § 87-302(a)(15).

233. These violations have caused financial injury to Plaintiffs and Class Members.

234. Accordingly, Plaintiffs, on behalf of themselves and Class Members, bring this action under the Uniform Deceptive Trade Practices Act to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and costs.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs pray for judgment as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Classes;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;
- C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Cyber-Attack and data breach;
- D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- E. Ordering Defendant to pay for not less than three (3) years of credit monitoring services for Plaintiffs and the Classes;
- F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- G. For an award of punitive damages, as allowable by law;
- H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- I. Pre- and post-judgment interest on any amounts awarded; and
- J. Such other and further relief as this court may deem just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs demand a trial by jury of all claims in this Complaint so triable. Plaintiffs also respectfully request leave to amend this Complaint to conform to the evidence, if such amendment is needed for trial.

February 24, 2021

Respectfully submitted,

/s/ Gary M. Klinger

Gary M. Klinger  
**MASON LIETZ & KLINGER LLP**  
227 W. Monroe Street, Suite 2100  
Chicago, Illinois 60606  
Phone: (202) 429-2290  
Fax: (202) 429-2294  
gklinger@masonllp.com

Gary E. Mason \*  
David K. Lietz\*  
**MASON LIETZ & KLINGER LLP**  
5101 Wisconsin Avenue NW, Suite 305  
Washington DC 20016  
Phone: (202) 429-2290  
Fax: (202) 429-2294  
gmason@masonllp.com  
dlietz@masonllp.com

*Attorneys for Plaintiffs and the Class*

\*Admission *pro hac vice* forthcoming